Noah Allen

PHIL375

12/4/2018

Banning Encryption

The history of encryption relates to humans' need for privacy of information. Humans have used various forms of communication as a vehicle for information. While animals and plants also communicate, humans have developed beyond the spoken word to develop writings, and beyond this into the digital age. As information is contained in human communications, also is the desire for people to keep certain information private – intended for themselves or others. A culture that speaks only one language cannot understand the language of another. If a human can develop their own way of communicating and establish this with another person or group, they can hide these communications from others. When written text is encoded in a certain manner, the way to decode the message can be known to an intended party. The same concept applies to digital communications, and encryption is a tool that can secure them. This paper will look at the history of encryption, and how it evolved from military to widespread public use. It will also look at some cases where the idea to ban, or outlaw, digital encryption has been proposed, and why it has not worked. Not only is it impossible to ban, encryption is important for freedom of the human spirit in the digital age.

A military application of encryption can be illustrated with an example from World War II. Poor encryption standards proved disastrous for Germans in the first world war, so superior methods of securing information were desired by the United States military during World War II.[1] During the second world war, the United States military recruited 29 Navajo Native Americas as "code talkers" to utilize a form of verbal encryption that enabled the military to communicate top secret information across long distances.[2] This worked because the "code talkers" were a small group, the only in the world, that spoke their language. This way, if a third party attempted to eavesdrop on a conversation, they would not be able to decipher it. In addition, the messages were double encoded, with the "code talkers" learning 200 new words for military use. In short, this utilization of the "code talkers" as a resource to communicate top secret information was a key element to the multiple successes for the United States military during the second world war.

As digital technologies progressed, the need for digital encryption was required for the protection of military secrets. Until the 1990's, all new encryption methods were considered munitions, and encryption techniques approved for public use could not be exported outside of the United States.[3] Because strong encryption standards were considered munitions, anyone who developed their own

---

[1] Andrew Lycett, "Breaking Germany's Enigma Code," BBC, last modified February 17, 2011, http://www.bbc.co.uk/history/worldwars/wwtwo/enigma_01.shtml.

[2] Eric Levenson, "The incredible story of the Navajo Code Talkers that got lost in all the politics," CNN, last modified November 29, 2017, https://www.cnn.com/2017/11/28/us/navajo-code-talkers-trump-who/index.html.

[3] Daniel Oberhaus, "How the Government Is Waging Crypto War 2.0," Vice, last modified August 10, 2016, https://motherboard.vice.com/en_us/article/jpgvy3/encryption-debate-the-end-of-end-to-end.

encryption method would be developing a munition. This actually occurred in the mid 1990's, when Daniel Burnstein, a mathematics professor, developed a new encryption method, the knowledge of which became forbidden.[4] The case wound up in the supreme court because the professor believed this was a violation of his freedom of speech. The court ruled in his favor – a pivotal reason for the shift of a ban on encryption methods, along with the United States relaxing its restrictions on encryption export controls.

In the early 1990's, the United States placed export controls on encryption. These restrictions hurt the business of companies seeking to utilize high-quality encryption because customers oversees were not able to get the best versions of software that companies were producing.[5] Imagine if a company has two versions of its products: one with high quality security, and another with weaker security that is more vulnerable to hackers. Customers oversees, receiving the lower-quality encryption variants of products, began feeling cheated. It was also costing companies money to have to develop two versions of their software, in addition to being time consuming and confusing trying to ensure they were following regulations. Such restrictions were argued to not even be effective – there was nothing stopping the knowledge of encryption from getting oversees to the countries the United States intelligence agencies were seeking to spy on.[6]

In the late 1990's, the Navy Research Labs developed a method of securely communicating through the public internet.[7] The technology was termed "onion routing" because it would encrypt data and route it through various layers like an onion, making it far more secure. The technology was released to the public in 2002, and development continued.[8] While the motivation for releasing this technology to the public is unclear, one of its uses is for journalists and whistleblowers of human rights violations in foreign countries to be able to protect their identity.[9] It can give freedom of speech in countries where this right is restricted. Another use is that it enables spies to communicate information back to the United States through the public channel of the internet, instead of having to bring sophisticated equipment.[10] This onion routing technology is widely in use worldwide, to this day; termed the "dark net". It is known to some to be the underworld of the internet, with people using it for anything from selling drugs, to human trafficking, selling personal information to identity thieves, and

---

[4] "Judge again finds encryption ban unconstitutional, issues stay," *Telecommunications Reports* 63, no. 35 (Sep 1997): 5, https://search-proquest-com.ezproxy.bellevuecollege.edu/abitrade/docview/216937354/53B9F9E803764774PQ/1?accountid=35840.

[5] Gary Anthes, "Group urges end of encryption export ban," *Computerworld* 25, no. 18 (May 1991): 88, https://search-proquest-com.ezproxy.bellevuecollege.edu/abitrade/docview/215944696/53B9F9E803764774PQ/7?accountid=35840.

[6] Ellen Messmer, "Encryption restrictions," *Network World* 21, no. 11 (Mar 2004): 69, https://search-proquest-com.ezproxy.bellevuecollege.edu/abitrade/docview/215962483/55B45295BE414590PQ/7?accountid=35840.

[7] "Private Web Browsing", Naval Research Laboratory, published June 2, 1997, https://www.onion-router.net/Publications/JCS-1997.pdf.

[8] Roger Dingledin, posting to web forum, September 20, 2002, http://archives.seul.org/or/dev/Sep-2002/msg00019.html.

[9] Cooper Quintin, "7 Things You Should Know About Tor," *EFF*, last modified July 1, 2014, https://www.eff.org/deeplinks/2014/07/7-things-you-should-know-about-tor.

[10] "The unlikely history of Tor," *ExpressVPN*, last modified February 14, 2018, https://www.expressvpn.com/internet-privacy/tor/history/.

horrendous abuses of women and children; a high price for giving people the unlimited access to a digital form of freedom of speech.[11]

In Paris, in 2015, the idea to ban encryption came into the social narrative after a highly publicized terror attack.[12] As a result, intelligence agencies called for a ban of encryption to prevent future terrorist attacks. However, there was no evidence that the attackers used encryption – the attackers did use Facebook and unencrypted text messages to communicate. Following this logic, all social media and text messages should be banned. Even if the attackers did use encrypted messages, the argument that encryption should be banned would still not hold because encryption is useful for many things that require privacy. A similar example is when Thresa May, London's Prime Minister, began calling for an end to encryption in response to a 2017 terror attack in London.[13] Her reasoning was that encryption technologies give terrorists the ability to communicate without getting caught. From her stance, if encryption is outlawed, then terrorists cannot have a safe place to conduct their communications, thus thwarting their ability to plan their attacks. This stance was met with great public opposition; it is a bad idea that does not work. Banning encryption is not a solution for terrorism. Encryption is used by basically everyone and necessarily for doing anything that requires privacy online – such as buying things or securing medical records. Furthermore, it would be far too difficult to enforce a ban on encryption because anyone can simply write their own encryption code.

An alternative to an outright ban on encryption is to give the government a backdoor, in the form of safely storing decryption keys, if they are needed by the government. This idea, known as "key escrow", does not work because hackers can figure out the backdoor, giving them a master key to hack everything.[14] In 2016, the *Feinstein-Burr Compliance with Court Orders Act* was proposed in the United States, set to require companies to put backdoors into their encryption systems, enabling government agencies to access encrypted information. Described by some as an anti-security bill, it also would have required all companies and individuals to provide data to the government in an intelligible manner when requested by a court order. Another way of explaining this bill is that it would have made it so any individual or company would be unable to have any digital communication or storage of data without the government being able to access it, if it desired to do so. The proposed bill faced great public opposition, gathering over 43,000 signatures in San Francisco, causing Congress to bypass it.[15] The way the law was written also would have required software creators to write their software in such a way to retain deleted files and hand them over to the government. It would have hindered the progress of security technologies and privacy as well as undermined innovation and public safety.

---

[11] Patrick Howell O'Neill, "Tor's ex-director: 'The criminal use of Tor has become overwhelming'," *cyberscoop*, last modified May 22, 2017, https://www.cyberscoop.com/tor-dark-web-andrew-lewman-securedrop/.

[12] Trevor Timm, "Paris is being used to justify agendas that had nothing to do with the attack," *The Guardian*, last modified November 20, 2015, https://www.theguardian.com/commentisfree/2015/nov/20/paris-attacks-political-agenda-immigration-encryption-surveillence.

[13] Timothy Revell, "Theresa May's repeated calls to ban encryption still won't work," *NewScientist*, last modified June 5, 2017, https://www.newscientist.com/article/2133644-theresa-mays-repeated-calls-to-ban-encryption-still-wont-work/.

[14] Frank Rietta, "U.S. Senate Bill Seeks to Ban Effective Encryption, Making Security Illegal," *Reitta*, last modified April 8, 2016, https://rietta.com/blog/2016/04/08/feinstein-burr-encryption-bill/.

[15] Iain Thompson, "US anti-encryption law is so 'braindead' it will outlaw file compression," *The Register*, last modified April 14, 2016, https://www.theregister.co.uk/2016/04/14/burr_feinstein_bill_prompts_protests/.

All attempts to ban encryption have failed. Today, the internet and the "dark net" remain an open forum of unregulated free speech; however, a creeping fear of censorship exists with the internet. The debate carries on about how to deal with problems that come with limitless freedom of speech in the digital realm. Encryption was ultimately allowed, after much effort to hold it back – but now, turning back is not an option. In other words, now that we have gone this far, there is no simple solution to fixing the problems that come along with the freedom that has resulted. Or, should society continue to live with these unsolved issues – viewing them as a cost to freedom? I think so. Of all the horrible things that can be found on the "dark net", it is free will that exposes somebody to them. Human curiosity and inquiry can be damaging, if handled foolishly. If there is one thing freedom of speech is good for, it is promoting the free exchange of information and ideas, which is also good for democracy. It can expose truth. This can liberate a society held captive to authoritarianism. The suppression of knowledge from outside sources is a tactic cults use to keep people enslaved. Psychologic experiments in the 1950's found that people faced with obvious evidence will not contradict the majority group most of the time, but once just one person in the group breaks the chain of conformity, its spell drastically diminishes in the others.[16] Once people become aware of things that are suppressed, and how their rights are being taken from them, a group awareness can form. The collective agreement of a group of people, seeking virtues of liberty and truth, can band together. This is dangerous to those who benefit from the suppression of others. Censorship can be a clever tool for the suppression of knowledge and ideas, and it can be utilized to manipulate a society. I believe it a bigger threat to the human spirit than anything that can be found on the "dark net".

[16] Martyn Shuttleworth, "Asch Experiment," *Explorable.com*, last modified February 23, 2008, https://explorable.com/asch-experiment.

Bibliography

Anthes, Gary. "Group urges end of encryption export ban." *Computerworld* 25, no. 18 (May 1991): 88. https://search-proquest-com.ezproxy.bellevuecollege.edu/abitrade/docview/215944696/53B9F9E803764774PQ/7?accountid=35840.

"Judge again finds encryption ban unconstitutional, issues stay." *Telecommunications Reports* 63, no. 35 (Sep 1997): 5. https://search-proquest-com.ezproxy.bellevuecollege.edu/abitrade/docview/216937354/53B9F9E803764774PQ/1?accountid=35840.

Levenson, Eric. "The incredible story of the Navajo Code Talkers that got lost in all the politics." *CNN*. Last modified November 29, 2017. https://www.cnn.com/2017/11/28/us/navajo-code-talkers-trump-who/index.html.

Lycett, Andrew. "Breaking Germany's Enigma Code." *BBC*. Last modified February 17, 2011. http://www.bbc.co.uk/history/worldwars/wwtwo/enigma_01.shtml.

Messmer, Ellen. "Encryption restrictions," *Network World* 21, no. 11 (Mar 2004): 69. https://search-proquest-com.ezproxy.bellevuecollege.edu/abitrade/docview/215962483/55B45295BE414590PQ/7?accountid=35840.

Oberhaus, Daniel. "How the Government Is Waging Crypto War 2.0." *Vice*. Last modified August 10, 2016. https://motherboard.vice.com/en_us/article/jpgvy3/encryption-debate-the-end-of-end-to-end.

O'Neill, Patrick. "Tor's ex-director: 'The criminal use of Tor has become overwhelming'." *Cyberscoop*. Last modified May 22, 2017. https://www.cyberscoop.com/tor-dark-web-andrew-lewman-securedrop/.

"Private Web Browsing", *Naval Research Laboratory*, published June 2, 1997, https://www.onion-router.net/Publications/JCS-1997.pdf.

Quintin, Cooper. "7 Things You Should Know About Tor." EFF. Last modified July 1, 2014. https://www.eff.org/deeplinks/2014/07/7-things-you-should-know-about-tor.

Revell, Timothy. "Theresa May's repeated calls to ban encryption still won't work." *NewScientist*. Last modified June 5, 2017. https://www.newscientist.com/article/2133644-theresa-mays-repeated-calls-to-ban-encryption-still-wont-work/.

Rietta, Frank. "U.S. Senate Bill Seeks to Ban Effective Encryption, Making Security Illegal." *Reitta.* Last modified April 8, 2016. https://rietta.com/blog/2016/04/08/feinstein-burr-encryption-bill/.

Shuttleworth, Martyn. "Asch Experiment," *Explorable.com*. Last modified February 23, 2008. https://explorable.com/asch-experiment.

"The unlikely history of Tor." *ExpressVPN*. Last modified February 14, 2018. https://www.expressvpn.com/internet-privacy/tor/history/.

Thompson, Iain. "US anti-encryption law is so 'braindead' it will outlaw file compression." *The Register*. Last modified April 14, 2016. https://www.theregister.co.uk/2016/04/14/burr_feinstein_bill_prompts_protests/.

Timm, Trevor. "Paris is being used to justify agendas that had nothing to do with the attack." *The Guardian.* Last modified November 20, 2015. https://www.theguardian.com/commentisfree/2015/nov/20/paris-attacks-political-agenda-immigration-encryption-surveillence.